MARKED-UP COPY OF ORIGINAL SPECIFICATION

[Description]

TITLE OF THE INVENTION

METHOD AND [ARRANGEMENT] SYSTEM FOR UPDATING A PASSWORD

BACKGROUND OF THE INVENTION

The invention relates to a method and [an arrangement] a system for updating a password.

Reference (1) discloses [such] a method and system such [an arrangement. In such an arrangement] that, if a user wants to use [this arrangement] the system, the user is asked to enter a password into the [arrangement] system. Once the password has been entered by the user, the [arrangement] system uses a database to check whether or not an entered password is a valid password for the user.

The [arrangement's] system's database stores a list containing permissible users of the [arrangement] system. Each user is allocated a respective password which is stored and has the entered password compared with it. Each password is also allocated a time statement. The time statement is used to indicate the period of time for which the password will be valid. If the period of time has elapsed, then the stored password becomes invalid, and the user is asked to update the password if he wants to use the [arrangement] system.

[This means that] The determination of whether the respective password is up to date, is made, to a certain extent, on the basis of the respective period of time, which ensures that the [arrangement] system has a higher level of protection against misuse or unauthorized ascertainment of a password. Reference (1) also discloses that the stated password can be

stored in the database in scrambled form (encrypted or formed using a one-way hash function). Reference (1) also discloses that the stated password can be transported in scrambled form via a communication link. An example of this is the Domain Logon in Windows NT. However, the time for changing the password is limited to the time of the login procedure.

Reference (2) discloses a communication standard, the H.235 Standard, in which boundary conditions, in particular message formats, can be exchanged between interconnected computers within the scope of multimedia communication.

The computers can be connected to one another logically or permanently.

A disadvantage of the methods disclosed in reference (2) is, in particular, that only static passwords can be used for a user.[, which means that] In this case, there is a relatively high likelihood of passwords stored in the computers being able to be ascertained and misused at some point in time by an unauthorized third party, a hacker.[, which means that] Therefore, the protection of the individual computers is no longer ensured.

Reference (3) discloses another communication standard, the H.225 Standard.

Reference (4) describes the so-called Abstract Syntax Notation 1 (ASN.1), which is used to define the format of a message within the context of the standards known from references (2) and (3).

An overview of protocols for updating cryptographic keys can be found in reference (5).

Particularly in the case of a large communication network having a multiplicity of interconnected computers, for example the Internet, the situation described above presents a high risk.

SUMMARY OF THE INVENTION

[The invention is thus based on the problem] In response to the difficulties and problems of specifying a method and [an arrangement] a system for updating a password between two interconnected computers, the present inventors propose a new method and a new system. [The problem is solved by the arrangement and the method having the features in accordance with the independent claims.]

The [A] method for updating a password between a first computer and a second computer has the following steps:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an

update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

[An arrangement] The system has at least one first computer and at least one second computer for updating a password between the computers,

the first computer and the second computer each having a processor which is set up such that the following steps can be carried out:

a) the second computer receives a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password,

b) the service request message from the first computer is used to request provision of a service,

c) the second computer checks whether the password contained in the service request message is valid for the first computer,

d) if the password is valid, the service is provided,

e) if the password is invalid, the second computer transmits to the first computer an update message which is used to request that the password be updated, and

f) the first computer and/or the second computer form an updated password which is subsequently used as the password within the context of the communication link.

[The] According to one aspect of the invention, [makes] it may be possible to update a password between two computers during a communication link existing between the two

computers. The second computer can distinctly force the first computer into having to update the password when the first computer is requesting a service from the second computer. [This means that the] The second computer thus ensures that the passwords are up to date, which increases the protection for communication between the computers. [Preferred developments of the invention can be found in the dependent claims.]

The developments described below apply both to the method and to the [arrangement] system; in the case of the development of the [arrangement] system, the respective processors in the computers are set up such that the development can be implemented.

In one development, the updated password is formed in the following manner:

a) the first computer transmits to the second computer a password message, containing the updated password, such that the updated password can be ascertained only by using the password,

b) the second computer uses the password to ascertain the updated password from the password message,

c) the second computer stores the updated password.

The second computer can transmit an acknowledgement message which is used to acknowledge the use of the updated password within the context of the communication link.

At the beginning of the method, the first computer is preferably authenticated by the second computer using an authentication token for the first computer, which is contained in the service request message. This increases the level of protection for the respective communication link.

In another refinement, the check to determine whether the password contained in the service request message is valid for the first computer is performed using a monitor database indicating for the first computer whether the second computer has already transmitted an update message to the first computer previously. This simplification makes the method faster to carry out, since a considerable computation time saving is obtained for the check.

The service request message preferably contains a statement relating to the integrity protection for the service request message, said statement being used by the second computer to check the received service request message for its integrity. The method is carried out only if the integrity of the service request message is ensured; otherwise, the requested service is refused. This further increases the level of protection for the respective communication link.

The password message contains the updated password preferably in encrypted form, the key for encrypting the updated password being formed on the basis of the password. This development creates a connection between the "old" password and the updated password.[, which means that] With the connection, perhaps only the owner of the password is actually able to ascertain the updated password. This improves the protection for the updated password when it is transmitted.

The key is preferably formed by stringing together the password a number of times.

Preferably, a plurality of first computers [is provided which] each have a password in common with the second computer, the password in each case being unique for the communication link between the respective first computer and the second computer. This [means that the invention can] allows for the method and system to be used very well in a large

communication network in which a server, the second computer, offers a plurality of clients, the first computers, services over the communication network.

In addition, a plurality of second computers can be provided which each have a password in common with each first computer, the password in each case being unique for the communication link between the respective second computer and the respective first computer.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of the present invention will become more apparent and more readily appreciated from the following description of the preferred embodiments, taken in conjunction with the accompanying drawings of which:

[An illustrative embodiment of the invention is shown in the figures and is explained in more detail below: In the figures]

Figure 1 shows a flowchart showing the method steps of the illustrative embodiment; and

Figure 2 shows a sketch showing computers which are connected to one another via a communication network.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings, wherein like reference numerals refer to like elements throughout.

Figure 2 shows a first computer 200 having a memory 202 and a processor 203 which are respectively connected to one another and to an input/output interface 201 via a bus 204.

The input/output interface 201 is used to connect the first computer 200 to a screen 205, to a keyboard 206 and to a computer mouse 207.

In addition, the first computer 200 is connected to other computers 210, 220, 230, 240 and 250 via a communication network 260, in the example an ISDN network (Integrated Services Digital Network).

The first memory 200 stores a database 208.

The other computers 210, 220, 230, 240 and 250 likewise have a respective processor 213, 223, 233, 243 and 253 and a respective memory 212, 222, 232, 242 and 252. The processor 213, 223, 233, 243 and 253 and the memory 212, 222, 232, 242 and 252 are respectively connected to the communication network 260 via a respective bus 214, 224, 234, 244 and 254 via an input/output interface 211, 221, 231, 241 and 251. In addition, the other computers 210, 220, 230, 240 and 250 are respectively connected to a screen 215, 225, 235, 245 and 255 and to a keyboard 216, 226, 236, 246 and 256 and to a computer mouse 217, 227, 237, 247 and 257.

Between the computers 200, 210, 220, 230, 240 and 250, the communication, i.e. protected interchange of multimedia data, takes place on the basis of the H.235 Standard, as described in reference (2).

The first computer 200 is in the form of a server and provides various services for the other computers 210, 220, 230, 240 and 250.

It is subsequently assumed that a second computer 210 wants to use a service from the first computer 200.

At the beginning of the method, a communication link is set up between the second computer 210 and the first computer 200 on the basis of the methods described in references (2) and (3). Once the communication link has been initialized, a logical connection exists between the second computer 210 and the first computer 200, i.e. the communication link has an associated logical channel which is uniquely identifiable. The logical channel is used to interchange messages 270, 280 between the computers 200, 210, 220, 230, 240, 250.

If the communication link has been set up, the second computer 210 can use a service from the first computer 200, in this case a database query for a database 208 stored in the memory 202 of the first computer 200. The text below describes the method which is carried out when the second computer 210 wishes to ascertain from the first computer 200 data from the latter's database 208.

A user of the second computer 210 enters the desired criteria for the database query into the second computer 210. The second computer 210 forms a service request message 101 (step 100) containing the criteria for the database query (cf. Figure 1).

The service request message 101 also contains the following variables:

- an authentication token permitting the second computer 210 to be authenticated by the first computer 200; the authentication token permits the password to be presented in a different form (for example in encrypted form or formed using a one-way hash function as one-way hash value);

- an H.235 address used to uniquely identify the first computer 200;
- a stated password PW for the user of the second computer 210.

For each other computer 210, 220, 230, 240 and 250, the first computer 200 stores a password associated with the respective computer 210, 220, 230, 240 and 250. If a service request message 101 formed by another computer 210, 220, 230, 240 and 250 contains a stated password which is the same as the stored password for the other computer 210, 220, 230, 240 and 250, then the requested service is granted to the user, i.e. is implemented by the first computer 200.

The password has a respective associated first time statement t1, used to indicate the time at which the password has been formed. The password also has a respective associated second time statement t2, used to indicate the period of time for which the password is valid.

The service request message 101 is transmitted from the second computer 210 to the first computer 200 (step 102).

Once the service request message 101 has been received in the first computer 200 (step 103), the second computer 210 is authenticated using the authentication token in the service request message 101 (step 104).

When the second computer 210 has been positively authenticated, the stated password PW is ascertained from the authentication token in the service request message 101 in a further step (step 105), and the stated password is compared with that password stored in the first computer 200 which is associated with the second computer 200 (step 106).

If authentication is negative, the service request message 101 is discarded (step 110),

and the requested service is not implemented.

If the stated password PW and the password associated with the second computer 200 match, then a check is carried out to determine whether the password is valid (step 107). This is done by ascertaining a current time t3 at which the service request message 101 has been received by the first computer 200.

If the stated password PW and the password associated with the second computer 200 do not match, then the service request message 101 is discarded (step 115), and the requested service is not implemented.

A check is carried out to determine whether the current time t3 is less than or equal to the sum of the first time statement t1 and the second time statement t2, that is to say whether the following rule (1) is true:

$$t3 \leq t1 + t2. \qquad (1)$$

If rule (1) is satisfied, [this means that] then the stated password corresponds to the password, and the password is still valid.

In this case, the service requested using the service request 101, that is to say the database query, is implemented by the first computer 200 (step 108), and the result of the database query is transmitted in a formed result message 116 (step 109) to the second computer 210 (step 110), in which the result of the database query is processed further (step 111).

If rule (1) is not satisfied, [this means that] then, although the authentication which has taken place authorizes the second computer 210 to request the service, in principle, the password associated with the second computer 210 is no longer valid.

In a further step (step 120), if a password is invalid, the first computer 200 forms an update message 121 and transmits it to the second computer 210 (step 122), said update message being used to request that the password be updated. In addition, the first computer 200 sets a bit (monitor value) to a first value in a monitor database, said value being used to indicate that the respective password is invalid and the appropriate update message 121 has been transmitted to the second computer 210.

When the update message 121 has been received (step 123), the second computer forms an updated password aPW (step 124).

If the second computer 210 does not keep to the prescribed procedure and generates a new service request without changing the password, then the first computer 200 is able to establish this after authentication of the second computer 210 and checking of the monitor value. If the monitor value has been set to the first value, the method can be terminated (step 131).

The updated password aPW is encrypted symmetrically on the basis of the Data Encryption Standard (DES). The key used to encrypt the updated password aPW is the password PW, which is also known and stored in the second computer 210.

The encrypted updated password aPW is transmitted to the first computer (step 127) in a password message 125 formed by the second computer 210 (step 126).

The password message 125 contains an integrity statement which can be used to check the integrity of the password message 125.

Once the password message 125 has been received (step 128), the integrity of the

password message (125) is checked (step 129).

If the integrity check is negative, the password message 125 is discarded (step 130), and the method is terminated (step 131).

If the integrity check is positive, the first computer 200 ascertains the encrypted updated password aPW (step 132), and the updated password aPW is decrypted (step 133).

In a further step, the ascertained updated password aPW is stored as the new password for the second computer 210 (step 134). In addition, the first computer 200 sets the appropriate monitor value in the monitor database to a second value, which is used to indicate that the respective password is valid.

Next, the first computer 200 forms an acknowledgment message 135 (step 136) and transmits it to the second computer 210 (step 137), and said acknowledgment message is received by the second computer 210 (step 138). The acknowledgment message 135 is used to acknowledge to the second computer 210 the further use of the updated password aPW within the context of the communication link.

In addition, the first computer 200 provides the service (step 108), forms the result message 116 (step 109) and transmits the result message 116 to the second computer 210 (step 110). In the second computer 210, the result message 116 is processed further (step 111).

The first computer 200 also sets the appropriate bit in the monitor database to a second value, which is used to indicate that the respective password is valid.

When another service request message is received, in each case after receipt thereof, the first computer 200 uses the monitor database to check whether or not the respective

password is valid. This allows the password to be checked very quickly.

The messages used within the context of this method [are] may be coded for example, on the basis of the H.225.0 Standard, as is described in reference (3).

To define the format (described below) of the individual messages, the Abstract Syntax Notation 1 (ASN.1), for example, described in reference (4) [is] may be used.

The messages are coded as a NonStandardMessage provided in reference (3), as described below:

```
NonStandardMessage ::= SEQUENCE
{
      requestSeqNum           RequestSeqNum,
      nonStandardData   NonStandardParameter,
      ...
      tokens                  SEQUENCE OF ClearToken OPTIONAL,
      cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
      integrityCheckValue     ICV OPTIONAL
}


NonStandardParameter ::= SEQUENCE
{
      nonStandardIdentifier   NonStandardIdentifier,
      data                          OCTET STRING
}


NonStandardIdentifier ::= CHOICE
{
      object                  OBJECT IDENTIFIER,
      h221NonStandard   H221NonStandard,
      ...
}


data ::= SEQUENCE
{
      alias             GatekeeperIdentifier,
      confirm                 boolean,

      -- optionally for the provision of integrity
      rejectReason            PWUpdateRejectReason    OPTIONAL,
      hash_algorithm          NonIsoIntegrityMechanism      OPTIONAL,
      token             HASHED OPTIONAL,
                              -- < alias, confirmation, new password>
      ...
}


PWUpdateRejectReason ::= CHOICE
{
      notregistered           NULL, -- keep the old password
      pw_wrong                NULL, -- keep the old password
      pw_old                  NULL, -- keep the old password
      ...
}
```

```
NonIsoIntegrityMechanism ::= CHOICE
{     -- HMAC mechanism used, no truncation, tagging may bei dem
necessary!
      hMAC-MD5                NULL,
      hMAC-iso10118-2-s EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (short MAC)
      hMAC-iso10118-2-l EncryptIntAlg,
      -- according to ISO/IEC 10118-2 using
      -- EncryptIntAlg as core block encryption algorithm
      -- (long MAC)
      hMAC-iso10118-3   OBJECT IDENTIFIER,
      -- according to ISO/IEC 10118-3 using
      -- OID as hash function (OID is SHA-1, RIPE-MD160,
      -- RIPE-MD128)
      ...
}


EncryptIntAlg ::= CHOICE
{     -- core encryption algorithms for RAS message integrity
      nonStandard       NonStandardParameter,
      isoAlgorithm            OBJECT IDENTIFIER,      -- defined in
ISO/IEC 9979
      ...
}


AliasAddress ::= CHOICE
{
      e164        IA5String (SIZE (1..128)) (FROM („0123456789#*,")),
      h323-ID     BMPString (SIZE (1..256)),
                  -- Basic ISO/IEC 10646-1 (Unicode)
      ...,
      url-ID      IA5String (SIZE (1..512)),
                  -- URL style address
      transportID TransportAddress,
      email-ID    IA5String (SIZE (1..512)),
                  -- rfc822-compliant email address
      partyNumber PartyNumber
}
```

A few alternatives to the illustrative embodiment described above are presented below:

The type of integrity protection is, in principle, arbitrary, as is the encryption algorithm for encrypting the updated password.

Providing the messages as nonstandard messages or nonstandard data field is not absolutely necessary. The messages may also be presented using protocol fields or messages which are to be newly defined, in the standards known from references (2) and (3).

The method and the [arrangement] system are also not limited to the standards known from references (2) and (3).

The service request message and/or the update message and/or the password message and/or the acknowledgment message can be formed separately as independent messages and can be transmitted separately between the computers which are involved. In addition, in one variant, the respective message can be transmitted between the computers involved together with other messages on the basis of the so-called "piggyback" principle.

By transmitting an update request to the first computer, the second computer can also request that the first computer form a new password. On a similar basis to the above comments, the second computer can use a monitor database stored therein and the appropriate monitor value to check whether the first computer has satisfied its request to change the password. In the negative instance, the second computer can abort the communication and terminate the method.

The following publications are cited in this document:

(1) Microsoft Developer Network Library, Questions 151082 S7D6D, S7590, S759E, S5970, Microsoft Press, July 1998, available on September 29, 1998 on the Internet at the following address:

http://msdn.microsoft.com/developer/

(2) International Telecommunication Union, Draft ITU-T Recommendation H.235, Line Transmission of Non-Telephone Signals, Security and Encryption for H Series (H.323 and Other H.245 Based) Multimedia Terminals), Version 1, Section 10.3.2, September 1997

(3) International Telecommunication Union, Draft ITU-T Recommendation H.225.0, Line Transmission of Non-Telephone Signals, Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems, Version 2, Sections 7.6 and 7.16, March 1997

(4) International Telecommunication Union, X.680 - X.683: OSI NETWORKING AND SYSTEMS ASPECTS - ABSTRACT SYNTAX NOTATION ONE (ASN.1), July 1994

(5) A. J. Menezes et al., Handbook of Applied Cryptography, CRC Press, New York, pp. 497 - 504, 1997, ISDN 0-8493-8523-7